Security Services versus Mechanisms

|  |  |
| --- | --- |
| **Security services/components/goals/features** | **Security mechanisms/methods/implementations** |
| the WHAT | the HOW |
| **Confidentiality**: The data d is only available to those that are authorized. | * Authentication (login, etc.)
* Authorization (file permissions)
* Encryption/decryption
 |
| **Data Integrity**: The user of data d trust that d is correct. | * Message Digest, checksums
* Message Authentication Codes (MAC)
* Digital Signatures
 |
| **Origin Integrity**: The user of data d trust that the origin data of d is correct. | * Message Authentication Codes (MAC)
* Digital Signatures
 |
| **Availability**: The service s is available to all that are authorized to use s. | * Replicated services
* Access Control
* …
 |
| **Non-Repudiability**: The actor of an action (A) cannot deny that he/she was the actor of that action. If the actor tries to deny that action, there exists an infallible mechanism to prove that he or she is lying. | * Digital Signatures
 |

Security Mechanisms and Prerequisites

|  |  |
| --- | --- |
| **mechanisms** | **Prerequisite(s)** |
| * Using Symmetric Cryptography to provide confidentiality
 | * Both the encryptor and the decryptor must have the key pre-shared. (This is usually accomplished by a key-exchange algorithm before the actual encryption/decryption take place.)
 |
| * (keyless) Message Digest
 |  |
| * Message Authentication Codes (MAC)
 |  |
| * Digital Signatures
 |  |
| * Digital Certificates
 |  |
| * SSL/TLS
 |  |
| * HTTPS
 |  |
| * Kerberos
 |  |
| * Diffie-Hellman
 |  |
|  |  |